2011 Mobile Threats Report

Published February 2012

TABLE OF CONTENTS

EXECUTIVE SUMMARY

In 2011, mobile malware reached a new level of maturity. Threats targeting smartphones and tablets are beginning to pose meaningful challenges to users, enterprises and service providers.

Mobile devices and apps have become critical to both personal and work life. Not only are they ubiquitous, but they are used for a breadth of experiences from entertainment and banking to critical business applications. In 2011, global mobile handset shipments reached 1.6 billion and tablet shipments reached 66.9 million.[2]

The sheer volume of mobile devices in use today has given rise to a staggering range of possibilities for users to interact with and manage their work and personal data while mobile. However, those same opportunities also open the door to hackers.

In 2011, Juniper Networks observed industrious hackers moving malware from proof of concept to profitability. Whether the motivation is notoriety, corporate espionage or financial gain, today's hackers are more sophisticated and chasing higher rewards in their attacks. This means sensitive information from businesses, governments, service providers and users is at greater risk.

Findings from the Juniper Networks Mobile Threat Center (MTC) in its 2011 Mobile Threats Report, compiled by Juniper security researchers, show three signs of this maturation:

- **There is more mobile malware than ever before.** In 2011, there was a record number of mobile malware attacks – particularly on the Google Android platform. The combination of Google Android's dominant market share and the lack of control over the applications appearing in the various Android application stores created a perfect storm, giving malware developers the means and incentive to focus on the platform.
- **Mobile malware has gotten smarter.** Malicious actors continue to hone their craft by finding new ways to exploit vulnerabilities and human behavior for profit across all mobile platforms and devices. In addition, the growing focus on security by researchers demonstrates the maturation of mobile security as an issue of concern for the business community as a whole.
- **There is a low barrier to entry.** Applications are turning out to be the "killer app" for hackers — and application stores are fast becoming the prime delivery mechanism for infected applications. Mobile users are downloading applications more than ever before. As we have seen a boom in the number of application developers, we have also seen a flood in the number of attackers. Juniper MTC data shows an evolution from more sophisticated, complex and deep attacks to attacks that are lightweight, fast, and application-based.

In addition to of the rising threat of malware, consumers and enterprises remain susceptible to a very low-tech yet devastating risk: stolen or lost devices. In the last year alone, nearly one in five users of Juniper Networks Junos® Pulse Mobile Security Suite, Juniper's comprehensive mobile security and device management solution, required a locate command to identify the whereabouts of a lost or stolen mobile device.[3]

Juniper MTC examined **793,631** applications and vulnerabilities across every major mobile device operating system to inform this 2011 Mobile Threats Report. Key findings and guidance, along with predictions about the evolving threat landscape, follow in this report.

JUNIPER NETWORKS MOBILE THREAT CENTER MALWARE DATABASE

To understand the numbers associated with mobile malware growth, it is imperative to have a firm understanding of the differences between mobile and PC-related malware.

In the PC world, malware commonly consists of spyware, Trojans, adware, worms and viruses. For mobile devices, the vast majority of malware is spyware and Trojans, which are either applications or functionality hidden within other applications. As such, gauging the amount and impact of mobile malware in 2011 is largely an exercise in analyzing, tracking and quantifying mobile applications.

Additionally, it is prudent to place mobile malware numbers in the proper perspective as compared to PC malware. Without question, the number of PC malware samples is drastically higher than those targeting mobile devices. One leading reason is that PC malware constantly needs to evolve to remain effective against the anti-malware capabilities available on or for most PCs.

Once PC security vendors discover malware, they add an identifying signature to detect it, essentially preventing the attack. To remain effective, the attacker must modify the malware to bypass signatures running on the vast majority of computers. This creates variants and subtle changes in the malware creating more samples.

Conversely, the vast majority of mobile devices do not yet deploy any endpoint anti-malware solution. To infect a mobile device, a malware writer needs only to create a malicious application, post the application to an application store and simply wait for users to unwittingly install their malware.

Mobile operating systems developers like Google and Apple are now able to remotely remove malware from devices that download it from official application stores and marketplaces, which is leading malware developers to create modified versions of common types of malware in order to elude removal. However, this mitigation does nothing for the millions of downloads from the web and third party app stores.

In 2011, the Juniper MTC analyzed 793,631 applications from numerous sources, including but not limited to:

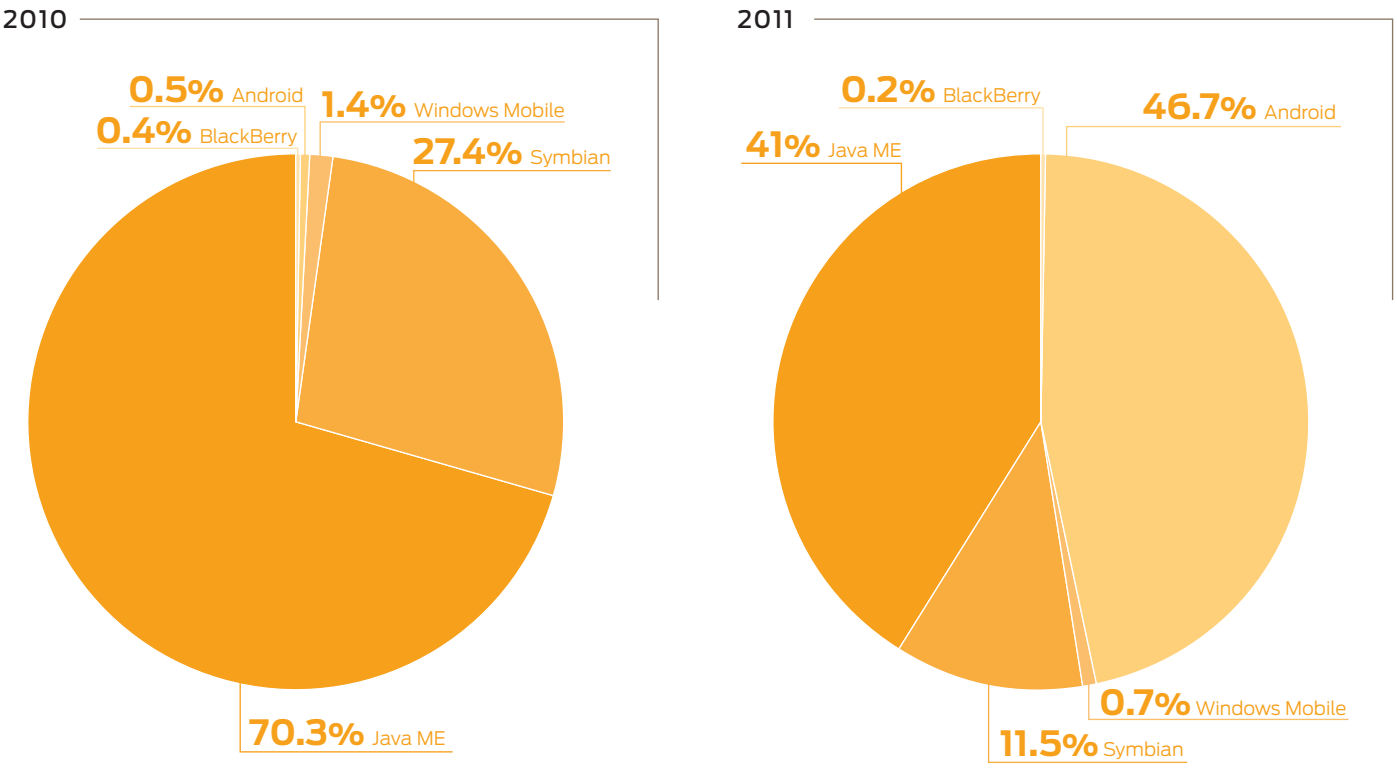
- Mobile operating system application stores
- Third-party application stores around the world
- Known website repositories of malicious applications
- Known hacker websites and repositories
- Application samples submitted by customers
- Application samples submitted by partners
- Applications identified “zero day” as malicious by Junos® Pulse Mobile Security Suite

The graph below is a comparison of unique mobile malware samples detected in 2010 and 2011 by the Juniper MTC. For the purposes of this report, Juniper MTC defines a mobile malware sample as a unique instance of malware or an application whose content or actions are deemed intentionally harmful or fraudulent by the MTC.

Prior to 2011, the vast majority of mobile malware was related to Nokia Symbian and Java ME devices, but in 2011, the Juniper MTC detected a substantial shift towards Android malware.

The Juniper MTC database does not include malware samples for Apple's iOS platform. This does not necessarily mean it does not exist or that the iOS platform is not vulnerable to malware. Indeed, there have been instances of applications pulled from Apple's App Store for violating Apple's terms of service. The inability to quantify iOS threats is largely due to Apple not releasing data or opening its platform for analysis.

UNIQUE MOBILE MALWARE SAMPLES DETECTED BY OPERATING SYSTEM



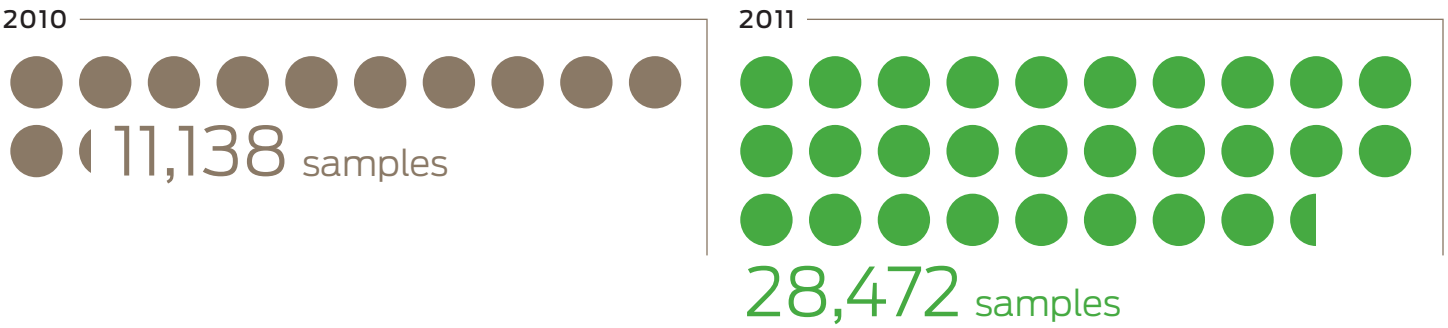
THE GROWTH OF MOBILE MALWARE

The rapid growth of mobile malware over the past few years demonstrates a significant level of maturity for this newly emerging threat to consumers and businesses. In 2011, the Juniper MTC identified a 155 percent increase in mobile malware across all platforms, as compared to the previous year.

This increase in mobile malware and the types of exploits used mirrors the growth and way people use mobile devices today. As more users adopt smartphones and tablets, and download millions of applications to do everything from gaming to social media or conducting financial transactions, cyber criminals have taken notice, and some have adjusted their attacks to follow these behavior changes.

In 2011, the Juniper MTC identified a 155 percent increase in mobile malware across all platforms, as compared to the previous year

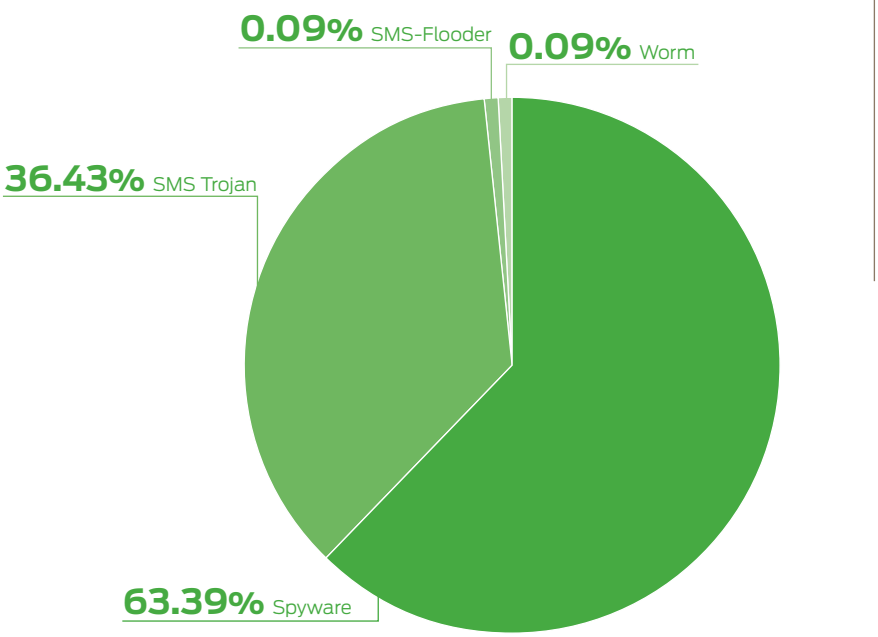
TOTAL MOBILE MALWARE SAMPLES ACROSS ALL OPERATING SYSTEMS



Types of Mobile Malware and How They Work

The vast majority of malware infecting smartphones and tablets can be classified into two categories: spyware and SMS Trojans. While profit is the major motive for both types of attacks, their design is fundamentally different.

TYPES OF MALWARE TARGETING MOBILE DEVICES



Spyware

In 2011, the Juniper MTC found that spyware was the dominant type of malware affecting Android, accounting for 63 percent of the samples identified. Spyware is an application that has the ability to capture and transfer data – such as GPS coordinates, text records or browser history – without providing an explicit means for the user to identify the application's actions. Ultimately, the captured data can lead to financial gain for the attacker and financial loss as well as an invasion of privacy for the device owner.

SMS Trojans

SMS Trojans, which according to Juniper MTC research, account for 36 percent of known mobile malware, run in the background of an application and clandestinely send SMS messages to premium rate numbers owned by the attacker. Once the message is sent, the money is not recoverable, and the owners of these premium rate numbers are generally anonymous. Examples of several types of SMS Trojans are detailed in the fake installer portion of this report.

Suspicious, but Not Malicious?

Along with outright malicious applications aimed at stealing information or money from victims, the Juniper MTC also detected a much larger number of suspicious applications that could pose privacy concerns or share unnecessary information with a third party. Several applications that were analyzed collect information or ask for a number of permissions that are over-reaching, dubious or unethical.

The following are some of the permissions that suspicious applications requested and the associated risks measured by the Juniper MTC:

- 30 percent of applications have the ability to obtain the device location without users' explicit consent
- 14.7 percent of applications request permissions that could lead to the initiation of phone calls without user knowledge
- 6 percent of applications requested the ability to look up all the accounts on the device, including email and social networking sites
- 4.8 percent of applications were able to send an SMS message without users' involvement and knowledge

Google Android: The Advantages and Risks of Popularity

The rapid rise in adoption over the past few years of the Google Android operating system has made it the most popular mobile operating system, unseating strong incumbents such as RIM's BlackBerry and Apple's iOS.

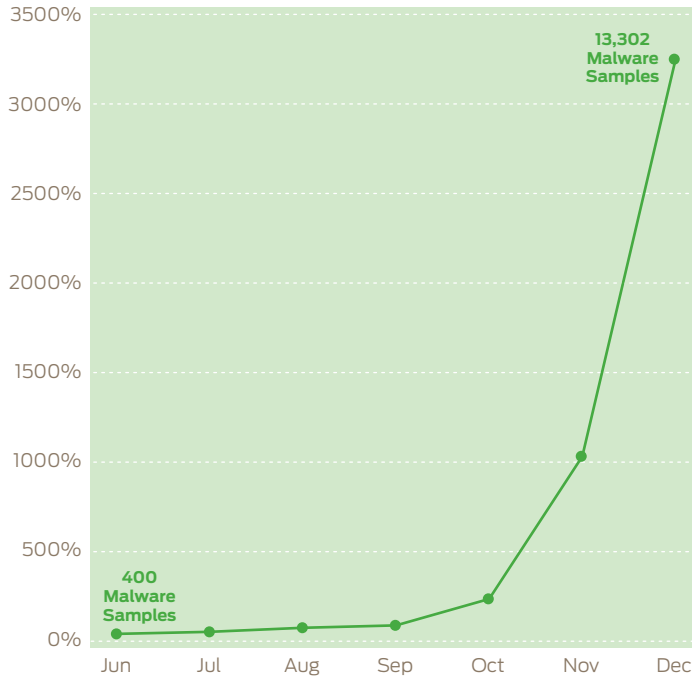
Since its release in 2007 to November 2011, Android grew its market share to a commanding 46.9 percent, compared to 28.7 percent for the iOS platform, its nearest competitor.[4] Further, the open nature of the Android platform and its application marketplace, the Android Market, made it easy for developers to bring new and useful applications to market quickly, with more than 500,000 Android applications published[5] and 10 billion application downloads.[6]

However, the same characteristics that have allowed Android to succeed have also created new risks. In the last seven months of 2011 alone Juniper MTC found, malware targeting the Android platform rose 3,325 percent to 13,302 samples.

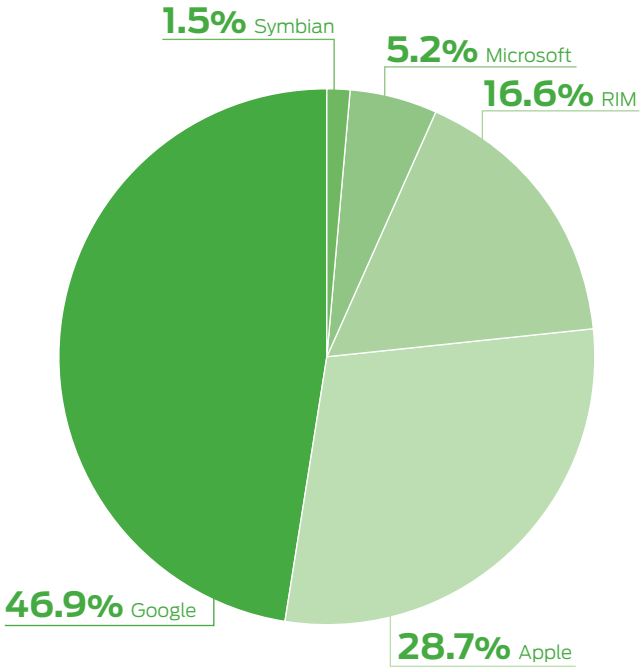
Potential attackers are looking to get the best return on their efforts and simply targeting the largest audience. Similar to the computing world, there is a clear link between market leadership and the attention of cybercriminals. Just as Microsoft Windows is the dominant market share leader in computer operating systems, it is also overwhelmingly the main target for malware. The same is now true for Google Android on mobile devices.

> In the last seven months of 2011 alone, malware targeting the Android platform rose 3,325 percent

CUMULATIVE ANDROID MALWARE INCREASE



MARKET SHARE OF SMARTPHONE SUBSCRIBERS BY PLATFORM



Another driver of Android-based attacks is Android's open application marketplace model, which makes it easier for attackers to reach potential victims. Currently, a developer can post an application to the official Android Market and have it available immediately, without inspection or vetting to block pirated or malicious applications.

Google has been diligent in quickly removing malicious applications from the official marketplace when found, but the process of detection and deletion can take days, providing more than enough time for successful attacks. Similar to "zero-day" attacks in the computer world, attackers know they are likely to get their exploits to market, even if only for a short time, which encourages more malicious development.

Complicating matters is the ability for Android devices to freely download applications from anywhere. While this grants users greater flexibility on their device, several unofficial third-party application stores have surfaced, filled with a mix of legitimate and malicious programs. Unlike the official Android Market, there is little to no effort to delete known malicious applications in third-party app stores. These third-party app stores are particularly popular in Eastern Europe and China.

Another security concern with Android is the availability of, and deployment time needed, for updates to the operating system. Android's open source model relies on mobile device manufacturers and service providers to push security patches through the devices. However, many device manufacturers build customized versions of the Android operating system and, as a result, certain devices do not receive – or must wait months to receive – security updates. This means that even patched security vulnerabilities and new security features may not get pushed to all devices, making them less secure and more vulnerable to malware.

RIM's BlackBerry and Other Platforms

In 2011, the Juniper MTC observed that malware targeting RIM's BlackBerry, Nokia's Symbian and other mobile operating platforms also continued to grow, albeit at a significantly lower rate than in previous years. Specifically, variants of the ZeuS Trojan (aka ZeuS-in-the-Mobile, or ZitMo) were found on BlackBerry devices. On BlackBerry devices infected by this malware, criminals obtained user credentials to initiate online banking sessions, giving the attacker access to the victim's financial accounts.

Similarly, for the other major mobile platforms, the threat of malware still exists. And, the threat is growing, although at a much slower rate than Android threats. New Java ME malware is still being identified and collected, with a 49 percent increase in incidents this year. Java ME-based applications are popular among Symbian and Windows Mobile devices, and can run across either platform.

The Juniper MTC collected 3,851 new malicious Java ME samples in 2011, showing that, while Symbian and Windows Mobile devices declined in market share as compared to Android and iOS devices, there are still enough users to hold the interest of Java ME malware developers.

MOBILE ATTACKS AND VULNERABILITIES GET MORE SOPHISTICATED

In addition to an increase in volume, the Juniper MTC saw malware grow significantly more sophisticated in 2011. For instance, in March, malware that was capable of leveraging existing platform vulnerabilities affected 85 percent of all Android devices, namely those running Android version 2.2.2 or earlier versions of the operating system. These vulnerabilities, coupled with the malware, enabled criminals to gain root access on the device and install additional packages to extend the functionality of the attack.

ATTACKS 2011: A YEAR IN REVIEW

JANUARY:
GEINIMI PROVIDES A SIGN OF COMPLEXITY TO COME

Geinimi was the first Android malware to leverage botnet-like capabilities and repackage legitimate applications with malware. These repackaged applications, primarily targeting games, were released in third-party application stores in Asia and were "sideloaded" by users to their Android mobile devices.

FEBRUARY:
ADRD GENERATES TRAFFIC

ADRD issued commands to Android devices to send HTTP search requests to specific addresses. The malware increased site rankings for a specific website, resulting in additional advertising revenue.

MARCH:
DROID DREAM CREATES A NIGHTMARE

Droid Dream infected legitimate applications in the official Android Market, affecting more than 50,000 users. By exploiting an existing vulnerability in the Android operating system, the malware gained root account privileges, and installed additional malevolent and dangerous code on the Android device without user intervention or knowledge.

MAY:
DROID KUNGFU MAKES A DISGUISED ATTACK

Droid KungFu leveraged two different exploits that enabled root access of Android devices through encrypted payloads so they could go undetected by malware scanning engines. The result of the attack provided the attacker with total control over the device.

JUNE–JULY:
THE RETURN OF DROID KUNGFU 2 AND 3

Droid KungFu gave way to Droid KungFu 2 (June) and Droid KungFu 3 (July), which contained malware that obfuscated their communications and code making it much more difficult for security experts to identify and stop the malware. Like their predecessor, it gave attackers total control over the device.

SEPTEMBER:
DROID DELUXE TARGETS USER ACCOUNTS

Droid Deluxe gained root access on infected Android devices, stealing email credentials, social network account information and banking login information. By leveraging the Android operating system's root permissions, Droid Deluxe was able to bypass existing security controls.

OCTOBER–DECEMBER:
FAKE INSTALLERS SIMPLY FOCUS ON MAKING MONEY

Between October and December, there was a sharp rise in fake installers (discussed later in this report), with an 872 percent increase in the number identified. This malware tricks users into paying via premium text messages for otherwise free or pirated versions of applications found in third-party application stores.

NOVEMBER:
iOS CODE SIGNING VULNERABILITY

A vulnerability in Apple's iOS platform allowed a security researcher to sneak an unreviewed application onto the official Apple App Store, proving it is possible to get malicious applications past Apple's app screening process.

JAN FEB MAR APR MAY JUN JUL AUG SEP OCT NOV DEC

source: Juniper Mobile Threat Center

Apple iOS Vulnerabilities

While malicious applications on the iOS platform are limited in large part due to Apple's closed application marketplace and stringent screening model, it does not necessarily make it fundamentally more secure. For one, when a user "jailbreaks" their device by removing the limitations on the operating system, the device can be susceptible to malicious applications downloaded from third-party sources.

Further, there are virtually no meaningful endpoint security products for the iOS platform because Apple does not provide developers with the tools to create them. This lack of software protection and a competitive security market leaves users with little protection if malware were ever to make it through Apple's application vetting process. In the long run, this could create a false sense of security for Apple users and prove to be an even bigger risk than Android's open model.

The Dangers of Jailbreaking Impostors

There are an increasing number of websites, such as JailbreakMe, that enable users to easily jailbreak their Apple devices by leveraging iOS vulnerabilities, allowing them to install any application on their device. However, as jailbreaking becomes more popular, several spoofed sites have surfaced that jailbreak mobile devices but also leave malware behind as part of the process. This gives the attackers access to personal information and root access to the iOS device.

A Chink in the App Store Armor?

In late 2011, Charlie Miller, a security researcher at Accuvant, found a technical way around Apple's application review process that allowed him to upload unapproved applications to the App Store.[7] Miller found a vulnerability in the code-signing restrictions – used to prohibit code not approved by Apple from running on iOS devices – which enabled him to run his own applications without approval.

Miller developed and posted a proof-of-concept application, demonstrating the security breach and possibility that malware could be developed for and propagated to the iOS platform. Apple eventually issued a fix for the issue. However, the episode was the most public disclosure to date that the iOS platform was vulnerable to attacks.

The ability for cybercriminals to develop similar attacks that are capable of getting around Apple's security measures, combined with the closed nature of the iOS platform and App Store, could eventually put its users at significant risk of attack. Apple prevents development of anti-malware applications for its devices, which limits the availability of a competitive security market for its platform. This means there is less innovation on security controls and no available protections for consumers against a potential malware outbreak.

Direct Attacks

Direct attacks consist of an attacking system or a user performing actions to exploit mobile device systems, components or interfaces. Common direct attack methods include:

- Sending malicious content or packets to device interfaces
- Sending malicious and malformed messages via SMS, MMS or email
- Attacking device applications with malicious content or packets
- Attacking vulnerabilities or misusing capabilities within a device browser

In 2011, security research focused more directly on vulnerabilities in the device browser that could be used for exploits. Specifically, research focused on vulnerabilities that enabled drive-by downloads, whereby downloads to the mobile device would begin automatically without the end-user taking action to do so.

Browser-Based Threats

The Webkit engine, used by iOS, Android, BlackBerry and webOS mobile browsers has several well-documented vulnerabilities that attackers are now targeting. Unlike application-based threats, which rely on users knowingly downloading an infected application, these browser-based attacks are triggered by simply visiting an infected website. Through a technique known as 'drive-by downloads,' unsuspecting users visit an infected website and malware begins downloading automatically without the end user's knowledge. For example, a Webkit vulnerability, known as CVE-2010-1807, allows remote attackers to execute arbitrary code or cause a Denial of Service (DoS) attack via a specially crafted HTML document, causing applications to crash.

At the Black Hat 2011 conference, researchers from Dasient Research presented a proof-of-concept attack that leveraged two previously discussed threat vectors.[8] First, they used known WebKit vulnerabilities in Android's browser to perform a drive-by download attack. Then, they leveraged a Skype application vulnerability to gain access to the user's Skype contact database on their mobile device and the information contained therein. Both of these exploits transpired on a device that was simply being used to surf the Web.

The basic steps to perform this attack include:

Step 1. The mobile device visits a malicious webpage.

Step 2. The malicious webpage exploits the device, which enables a connection between the mobile device and the attacker.

Step 3. The attacker sends commands to obtain data from the mobile device. In this case, the data messaged information available via a vulnerability in the Skype application.

Step 4. The Skype data is stolen by the attacker.

Dasient Research's proof of concept presentation demonstrated what the Juniper MTC believes will be a major trend in direct attacks in the coming years – leveraging a combination of weaknesses in applications and vulnerabilities in browsers or operating systems to gain access to sensitive data on a mobile device.

LOW BARRIER TO ENTRY DRIVES ATTACKS

In addition to an exponential increase in mobile malware as well as in its sophistication, there is now a low barrier to entry for attacks. Consumers and business users are downloading more applications than ever before with little consideration of potential security concerns. As a result, applications are turning out to be the "killer app" for hackers, making it easy for them to exploit unsuspecting users.

Juniper MTC data shows an evolution of many attacks, moving from more sophisticated, complex and deep attacks to lightweight, fast, application-based threats that rely on social engineering to trick users into either paying for pirated or otherwise free applications. These schemes require much less technical skill than the more complex attacks, which require deep understanding of security vulnerabilities. As a result, there is a low barrier to entry and a rapid growth in these types of exploits.

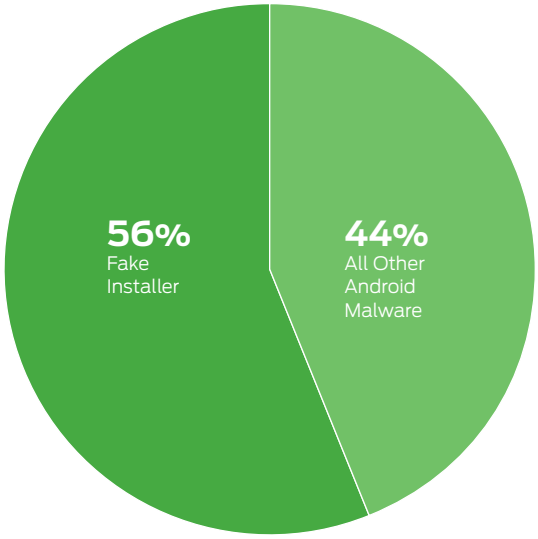
Social Exploits: Fake Installers

In October 2011, the Juniper MTC started to find large numbers of malicious applications called fake installers in several third-party application stores. These fake installers exploited user ignorance rather than technical vulnerabilities. These new pieces of malware operate as SMS Trojans that trick users into agreeing to automatically send premium text messages to attackers when downloading either pirated versions of paid applications or applications that could be otherwise found free on the official Android Market.

Compared to some of the more complex malware variants that surfaced in 2011 – which required a significant investment in development and dissemination – this malware is open to both expert and novice criminals, and presents a low barrier to entry. Furthermore, the use of premium SMS messages presents an easy way to make a quick and direct profit versus needing to find a way to monetize ill-gotten personal information.

These applications underscore the need for consumers to be very careful about where they obtain or purchase their applications and the app stores they use. In addition, if any application asks a user for a payment via SMS, they should exercise additional caution.

FAKE INSTALLER VS. ALL OTHER ANDROID MALWARE

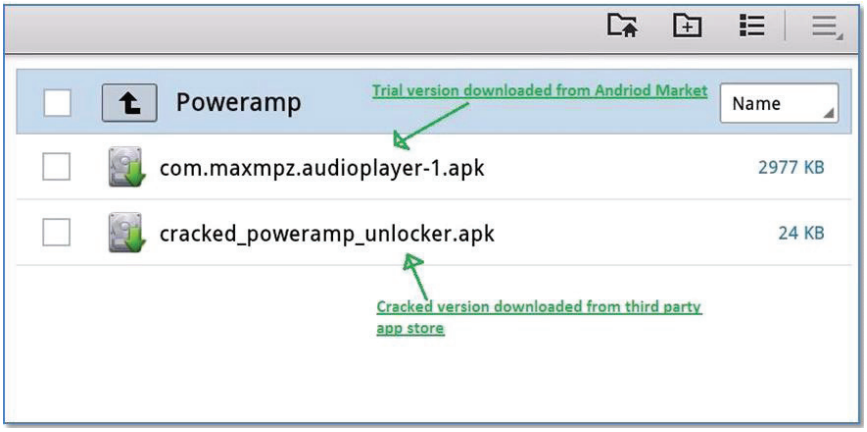


Fake Installer Example 1: Pirated Applications

In several cases, the Juniper MTC found malware authors distributing "cracked" or pirated versions of paid applications, diverting payments from legitimate developers. In one case, the MTC found a cracked version of a prominent paid media player application, PowerAMP, for download on third-party app stores. To the end user, the pirated version of PowerAMP worked exactly like the full, paid version of the app; but instead of paying the legitimate app developer, funds were diverted to the cybercriminal.

When visiting a third-party application store, the victim found a pirated version of PowerAMP that looked like the official version of PowerAMP, and were then prompted to pay for it by agreeing to have premium SMS messages automatically sent from their mobile device to a number linked to the hacker masquerading as the developer.

TRIAL AND CRACKED COPY OF POWERAMP ON AN ANDROID DEVICE



Fake Installer Example 2: Opera Mini

The majority of fake installers trick users into paying for otherwise free applications and send profits back to the fraudsters through premium SMS messages. In the case of the fake Opera Mini Web browser application, attackers tricked users into paying the price of three premium SMS messages when the user could have easily downloaded the application free from the Android Market.

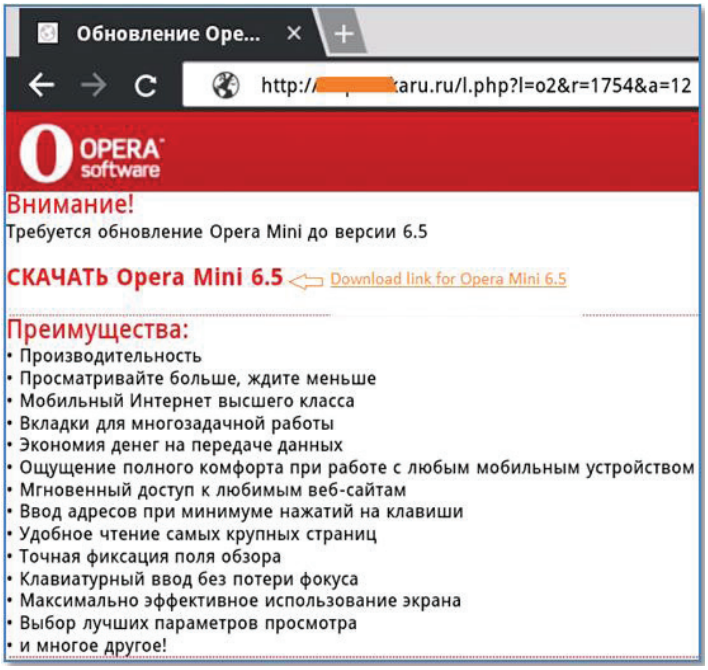
The following table provides information on the permissions requested by the fake Opera Mini Web browser application, along with its MD5 hash:

Name	Opera Mini 6.5
MD5	f0ec0e71c49083ad59e766697f39ecb4
Permission	android.permission.SEND_SMS android.permission.CALL_PHONE android.permission.RECEIVE_WAP_PUSH android.permission.READ_SMS android.permission.RECEIVE_WAP_PUSH android.permission.INTERNET

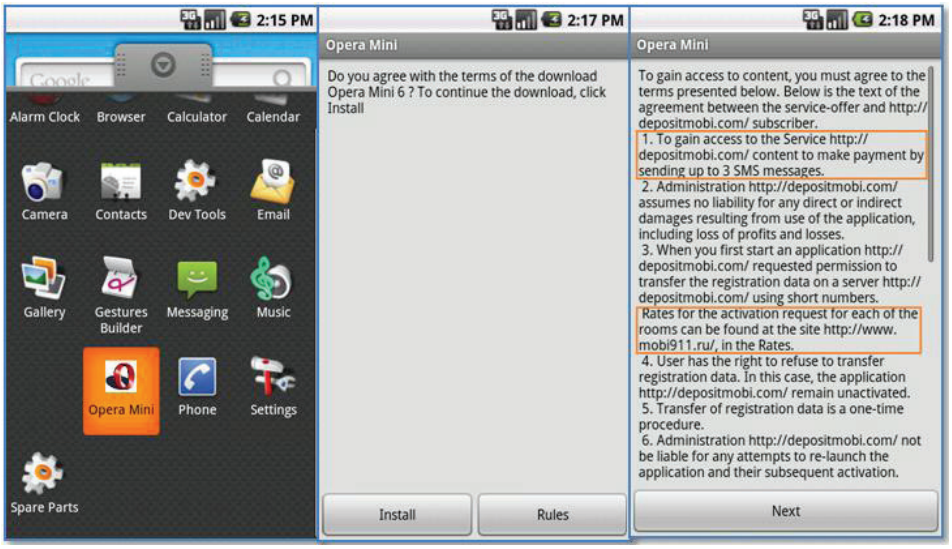
STEP-BY-STEP OVERVIEW OF THE MALICIOUS APPLICATION

Step 1: Android user receives a link to a third-party mobile app store via SMS or in an email.

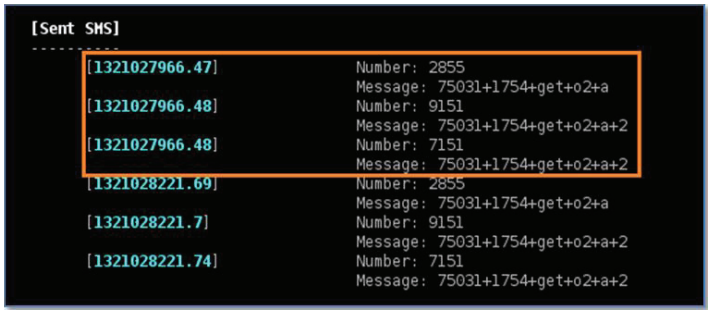
Step 2: The user tries to open the link on an Android device but is redirected to a website that informs the user to upgrade Opera Mini Web browser for Android to the latest version, which is 6.5:



Step 3: Upon accessing this application, the user receives a message that informs them that in order to download the Opera Mini 6.5 Web browser, they must pay for the service by sending three SMS messages:



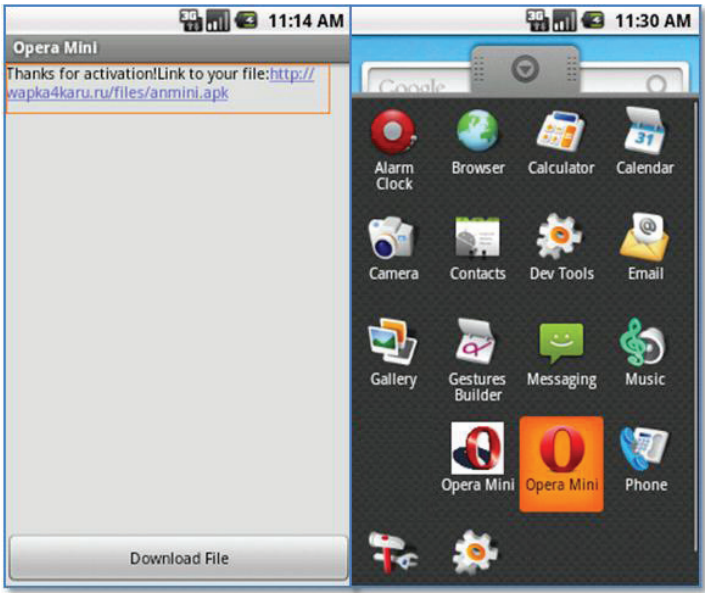
Step 4: If the user clicks on "Install," the application sends three SMS messages to premium numbers. The captured SMS messages are shown here:



COST PER PREMIUM SMS MESSAGE:

Premium Numbers	US $	Rubles (Russian Currency)
2855	6.65	203.2
9151	3.32	101.6
7151	1.1	33.87
Total	**11.07**	**338.67**

Step 5: After misapropriating the money, the fake Opera Mini application reveals the download URL that hosts the actual Opera Mini Web browser application:



In just about every case of a fake installer, funds are non-recoverable. The onus falls on the user to pay the bill at the end of the month or to dispute the bill, potentially forcing the service provider to shoulder the cost.

Connectivity Hacks

Network communications are vulnerable to compromise if not properly secured. However, this type of attack has historically required deep expertise and significant time investment on behalf of the criminal. Today, however, that has changed with the popularity of smartphones and tablets. These devices frequently rely on public, and typically unsecure, Wi-Fi access, which makes them susceptible to attack. Following analysis, the Juniper MTC found that two prominent threats emerged, Wi-Fi hacking and man-in-the-middle (MITM) attacks.

Wi-Fi Hacking

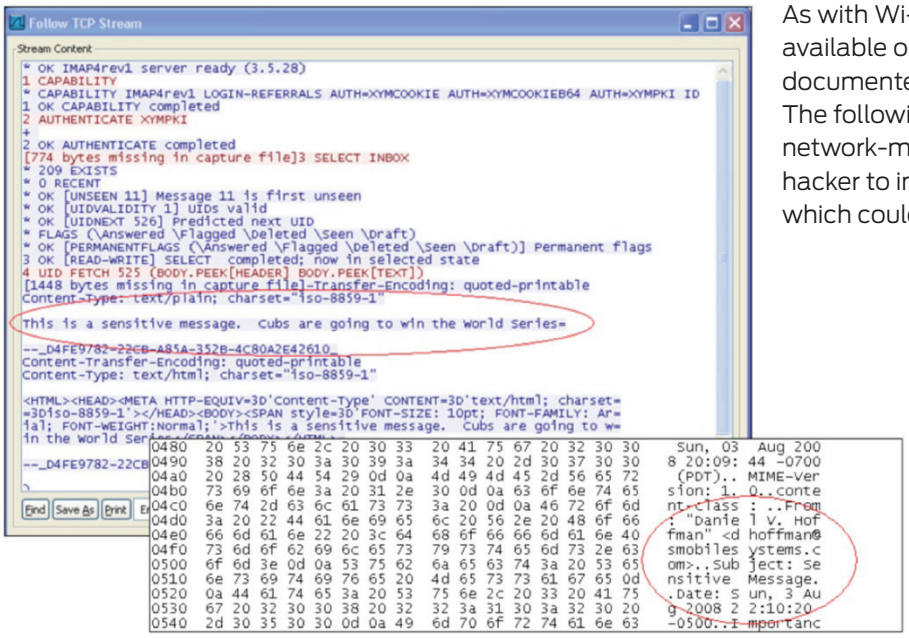
Given the growing adoption of Wi-Fi-enabled smartphones and tablets, the number of Wi-Fi hotspots globally is expected to grow from 1.3 million in 2011 to 5.8 million by 2015, representing a 350 percent increase.[9] Public Wi-Fi hotspots represent a very easy channel for hackers to exploit. With tools such as FaceNiff and Firesheep, finding users on a Wi-Fi network, hijacking the users' credentials, and using those credentials to impersonate a user online is now simply a matter of clicking on an icon. In an instant, attackers can steal passwords, leading to financial consequences and, in many cases, identity theft.

KEY DATA COMMUNICATIONS INTERCEPTION FINDINGS

- Wi-Fi hotspots expected to grow 350 percent by 2015
- Widely available tools make it simple to hijack users' credentials from Wi-Fi networks

Man-in-the-Middle Attacks

Wi-Fi networks are also susceptible to MITM attacks. When executing a MITM attack, hackers insert themselves into the communication stream from a mobile device connected to an unsecure Wi-Fi network, logging the information relayed between entities. Given many mobile devices submit communications in clear text, these attacks can provide criminals with access to a wide range of sensitive user and corporate information.



As with Wi-Fi hacking, MITM attack tools are widely available online and the methodologies are well documented on websites such as ethicalhacker.net. The following provides an example of how a common network-monitoring tool called Wireshark enables a hacker to intercept the emails of a mobile phone user, which could contain sensitive and valuable information.

MOBILE DEVICE MANAGEMENT: LOSS, THEFT AND HUMAN BEHAVIOR

Malware, connectivity and other technical threats only represent one aspect of mobile security. An equally important – if not more important – aspect is managing the potential loss, theft or misuse of a mobile device, and the data on the lost, stolen or misused device. There are also other behavioral concerns with mobile devices like keeping a child safe from unwanted content or contact.

Lost and Stolen Devices

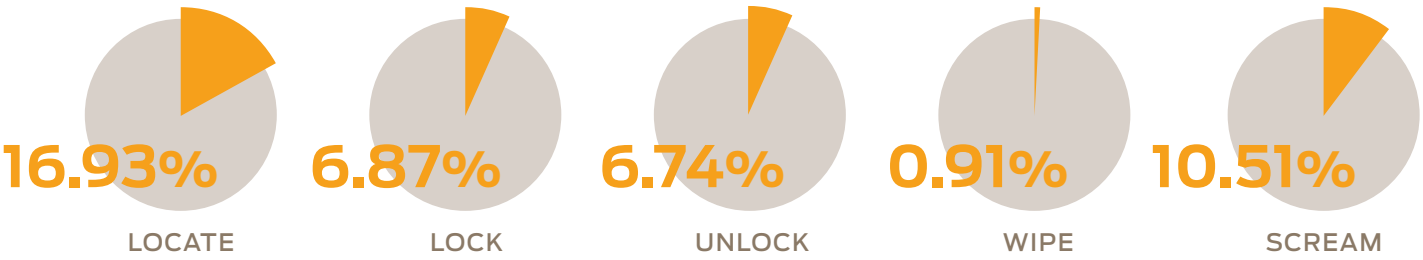
Chief among mobile device management (MDM) concerns is mitigating damage caused by a lost or stolen device, especially when that device contains sensitive corporate or personal information. A lost or stolen device, especially those without security settings like passwords, can present a significant risk to enterprises and consumers, including:

- **Data breach:** Like a laptop, a lost or stolen mobile device with customer or employee information can result in a data breach that may carry significant legal and reputational costs.
- **Loss of intellectual property and trade secrets:** Mobile devices often hold sensitive information about projects, as well as intellectual property, that if it falls in the wrong hands could have devastating effects on business.
- **Loss of personal information:** Mobile devices hold significant amounts of personal information, which if stolen could be used for a variety of malicious purposes, including fraud and identity theft.

Data gathered from Juniper Networks Junos Pulse Mobile Security Suite customers illustrates just how often mobile devices are lost or stolen. Over the course of 2011, nearly 1 in 5 (16.93 percent) of Junos Pulse Mobile Security Suite users issued the 'locate' command to find a missing device. Further, more than six percent needed to remotely lock those devices to guard against their inappropriate use.

Statistics also show a low rate of wipe commands compared to other actions available. Rather than immediately wiping a lost or stolen device, users have utilized the ability to visually display the device's locations in an online map or to initiate a "scream" command to cause a loud audible tone to emanate from a device within their vicinity. Having these steps available has led to device recovery, as opposed to device replacement, which has significant benefits to businesses and consumers.

REMOTE DEVICE MANAGEMENT: INCIDENCE OF CAPABILITIES USED



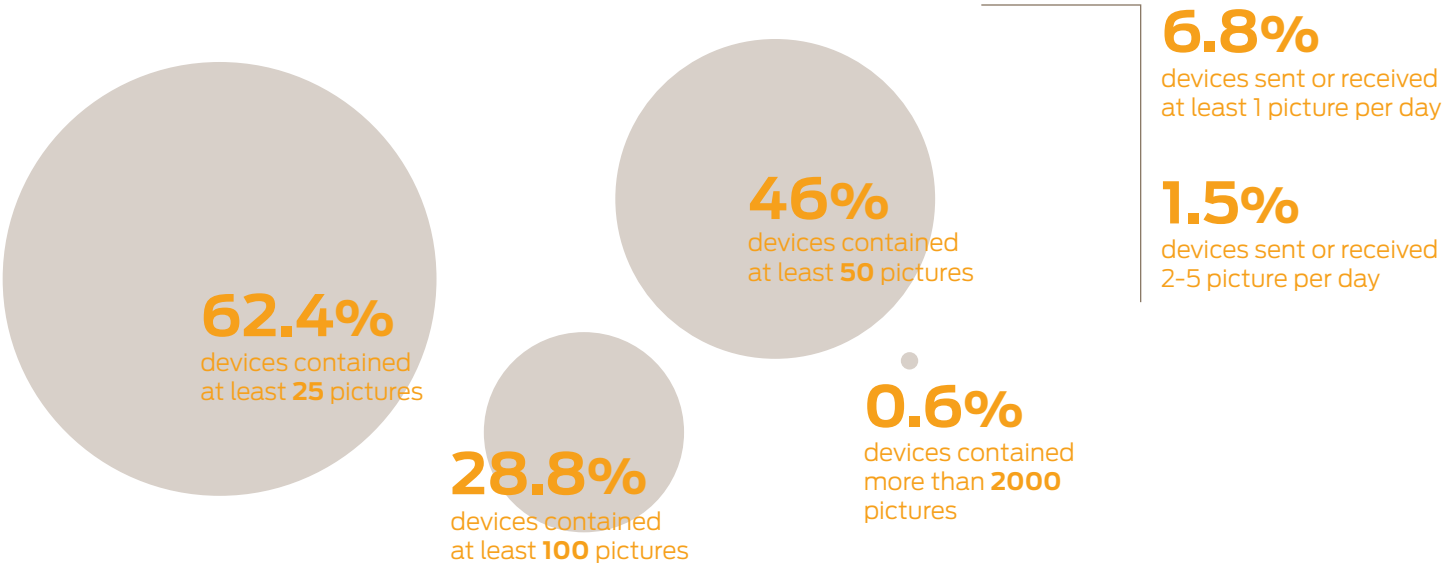
Child Online Safety and Parental Controls

Mobile devices have also become ubiquitous in the lives of today's teens and pre-teens. The use of social media, smartphones and the combination thereof creates an environment that is fertile ground for abuse, sexually inappropriate behavior and cruelty.

In fact, 58 percent of 14-to-24 year olds have experienced abusive behavior online,[10] and one-million children have been the victims of cyberbullying.[11] Further, approximately 10 percent of children between the ages of 10 and 17 years old have reported appearing in, creating or receiving sexually suggestive images.[12]

These trends when combined with anonymized data about child photo use compiled from a sampling of approximately 10,000 customers using Juniper's Junos Pulse Mobile Security Suite parental control features, underscores the need for parents to consider monitoring the content sent and received on their child's mobile device.

Key factors in protecting children from the threats associated with constantly being online via mobile devices requires parents to understand the threats and be enabled to monitor and control undesirable activity. Quality parental control products will enable parents to view and report on a child's SMS and email content, view pictures taken, sent and received by a device as well as monitor call logs.



A LOOK AHEAD: THE EVOLVING THREAT LANDSCAPE

Device technologies and applications, user behaviors, criminal operations and approaches, and even geopolitical factors all play a significant role in mobile device security. With all of these factors continuing to change with increased rapidity, the time for mobile device exploitation has truly arrived.

Looking to 2012, the Juniper MTC foresees:

- **Further dramatic malware growth.** In 2011, mobile malware reached a new level of maturity. With significantly more malware than ever before, threats became more sophisticated and the barrier to entry continued to remain low. In 2012, mobile device users can expect to see a dramatic increase in malware and notable advancements in malware-related attacks, particularly on the Android platform. Included in the nefarious malware advancements, the Juniper MTC expects to see a rise in complex mobile botnets and notable breaches in data security stemming from compromised mobile devices. Google's recent announcement that it will scan the Android Market for malware will also lead to an increase in malicious applications found on third-party markets, as well as an increase in malware variants attempting to bypass these new security measures within the Android Market.

- **Targeting of device applications.** As specific applications become widely adopted and standardized across mobile devices, the applications themselves will become the targets of attack. This is very similar to what occurred in the PC space, where document reader and office productivity applications are exploited as a means to obtain device data or remote control over the computing device.

- **Increased malicious focus on mobile banking applications and transactions.** Today's users utilize their mobile devices for everything from banking to online payments. As users become reliant on their mobile devices as digital wallets, this creates a very lucrative target for hackers.

- **Direct attacks via drive-by download and browser exploits.** Just as Web browsers have been a proven means of attack for PCs, the Juniper MTC has already started to see incidents where mobile browsers can be effectively targeted for exploits or as catalysts for an exploit. In 2012, there will be a concerted effort on the part of malicious individuals to attack the mobile browser as an entry point to compromise a device.

GUIDANCE: STEPS FOR USERS TO PROTECT THEIR "MOBILE LIFE"

For Individuals

In order to better protect their mobile devices, data and privacy from growing mobile malware threats, Juniper recommends the following steps for consumers:

- Install on-device anti-malware solutions to protect against malicious applications, spyware, infected secure digital (SD) cards and malware-based attacks.
- Install an on-device personal firewall to protect mobile device interfaces from direct attack.
- Utilize password protections for mobile device access, such as enforcement of strong passwords, password expiration dates, maximum password age and number of password attempts before initiating a remote device wipe.
- Use caution when downloading applications. While malware-infected applications have shown up in approved app stores and markets, it is still best to avoid third-party application stores whenever possible and only download applications from officially sanctioned sources.
- Install remote locate, track, lock, wipe, backup and restore software to retrieve, protect or restore a lost or stolen mobile device and the personal data on that device.
- Use anti-spam software to protect against unwanted voice and SMS or MMS communications.

For Parents

To protect against cyberbullying, sexting, cyberstalking, inappropriate use and other online threats, it is important that parents utilize device monitoring software that includes automated alerts for and visibility into:

- SMS message content
- Email message content
- Pictures taken, sent and received by their child's device
- Newly-installed applications
- Address book and contact lists
- Phone call logs
- Device location

For Enterprises

When implementing a mobile security solution, Juniper recommends that enterprises, government agencies and small-and-medium-sized businesses implement the following components:

Connect

- An SSL VPN client to effortlessly protect data in transit, and to ensure secure and appropriate network access and authorization
- A solution that integrates with network-based technologies, such as network access control (NAC), to determine appropriate access rights based on user identity and device security posture

Defend

- Support for all major mobile platforms, including Google Android, RIM BlackBerry, Apple iOS , Microsoft Windows Mobile and Nokia Symbian
- On-device anti-malware to protect against malicious applications, spyware, infected SD cards and malware-based attacks on the mobile device
- Centralized remote locate, track, lock, wipe, backup and restore facilities to retrieve, protect or restore a lost or stolen mobile device and the corporate data on that device
- On-device host checking to assess device security posture including device, OS version and malware status, patch and jailbreak/rooted status
- On-device firewall to protect mobile device interfaces

Manage

- Centralized administration to enforce and report on security policies across the entire mobile device population
- Device monitoring and control, such as the monitoring of messages (SMS and MMS), and control over installed applications and the installation of new apps
- Management capabilities to enforce security policies, such as mandating the use of PINs/passcodes, as well as defining and enforcing device passcode strength, expiry, maximum passcode age, number of passcode attempts before initiating remote device wipe, and more
- Ability for an administrator to monitor device activity for data leakage and/or inappropriate use

ABOUT THE JUNIPER NETWORKS MOBILE THREAT CENTER

The Juniper Networks Mobile Threat Center (MTC) is the only "CERT-style" organization in the world that conducts around-the-clock security, vulnerability and malware research tailored specifically to mobile device platforms and technologies. The Juniper MTC features highly skilled security professionals who have earned well-known industry certifications, including Certified Information Systems Security Professional (CISSP), Certified Ethical Hacker (CEH), Certified Hacking Forensic Investigator (CHFI), and GIAC Reverse Engineering Malware (GREM). Juniper MTC research team members are experienced corporate, military, government and academic professionals with decades of expertise in designing, building, managing, securing, attacking and auditing networks and devices.

Through its relationships and partnerships, the Juniper MTC gathers information and resources for analysis, then applies a proven, methodology-driven analysis of security concepts to mobile devices and operating systems. It leverages security concepts and advances relating to the three primary pillars of information security – confidentiality, integrity and availability – and applies them to the dynamic mobile device market. Juniper MTC team members are active members of and presenters at local and national security organizations, as well as participants on boards designed to guide the creation of mobile security community intelligence sharing capabilities. Based out of the Juniper Networks Mobile Center of Excellence located in Columbus, Ohio, the Juniper MTC consists of four teams:

- **Malware Research Team:** Identifies new mobile malware threats and device exploits.
- **Exploit Resolution and Integration Team:** Works with the Malware Research Team and other Juniper Networks development teams to create cutting-edge mobile security features and technologies and incorporate those solutions into Juniper Networks products, including the Junos Pulse Mobile Security Suite.
- **Device Analysis Team:** Analyzes new devices to identify platform vulnerabilities. Where necessary, the team ethically discloses any findings or research to the appropriate vendor in order to address platform or application vulnerabilities that could lead to exploit or compromise.
- **Device Testing Team:** Conducts testing of threat resolutions, new virus signatures and performance of Juniper Networks products across various device platforms.

For more information on the Juniper Networks Mobile Threat Center, visit **http://www.juniper.net/security/**

About the Junos Pulse Mobile Security Suite

Junos Pulse Mobile Security Suite delivers comprehensive mobile security and device management, securing most mobile devices, mobile operating system platforms, and the apps and data on mobile devices from malware, viruses, unwanted intrusion, and spam, while protecting against threats associated with device loss or theft. Junos Pulse Mobile Security Suite also manages and controls mobile devices and their apps, enabling or disabling certain features, allowing or disallowing specific applications, and remotely enforcing security policies on a user's mobile device, regardless if it is a personal or business-issued mobile device. When deployed in concert with Juniper's award-winning, market-leading SSL VPN gateways, Junos Pulse and the Junos Pulse Mobile Security Suite deliver secure, role-based mobile remote network and application access, providing the strongest security for data-in-transit available. Junos Pulse and the Junos Pulse Mobile Security Suite connect, protect, and manage mobile users, devices, their applications and data.

For more information on the Junos Pulse Mobile Security Suite, visit **http://www.juniper.net/us/en/products-services/software/junos-platform/junos-pulse/mobile-security/.**

REFERENCES

1 Strategy Analytics, "Global Handset Shipments Reach 1.6 Billion Units in 2011", January 26, 2011, **http://www.strategyanalytics.com/default.aspx?mod=pressreleaseviewer&a0=5169**

2 Strategy Analytics, "Android Captures Record 39 Percent Share of Global Tablet Shipments in Q4 2011," January 26, 2012, **http://www.strategyanalytics.com/default.aspx?mod=pressreleaseviewer&a0=5167**

3 Information obtained from analysis of Junos Pulse Mobile Security Suite infection reporting/alerting

4 comScore MobiLens, "comScore Reports November 2011 U.S. Mobile Subscriber Market Share", December 29, 2011, **http://www.comscore.com/Press_Events/Press_Releases/2011/12/comScore_Reports_November_2011_U.S._Mobile_Subscriber_Market_Share**

5 T3, "Android Market reaches 500,000 app mark", 2011-10-23, **http://www.t3.com/news/android-market-reaches-500000-app-mark**

6 wired.com, "Google's 10 Billion Android App Downloads: By the Numbers," Christina Bonnington, December 8, 2011 **http://www.wired.com/gadgetlab/2011/12/10-billion-apps-detailed/**

7 Forbes, "iPhone Security Bug Lets Innocent-Looking Apps Go Bad", July 7, 2011, **http://www.forbes.com/sites/andygreenberg/2011/11/07/iphone-security-bug-lets-innocent-looking-apps-go-bad/**

8 Dasient, "Mobile Malware Madness and How to Cap the Mad Hatters: A Preliminary Look at Mitigating Mobile Malware," July 2011, **http://www.dasient.com/mobile-malware-madness/**

9 TabTimes, "Smartphone and tablet adoption to drive increasing number of Wi-Fi hotspots," Doug Drinkwater, November 9 2011, **http://tabtimes.com/news/ittech-stats-research/2011/11/09/smartphone-and-tablet-adoption-drive-increasing-number-wi-fi**

10 2009 AP-MTV Digital Abuse Study, **http://www.athinline.org/MTV- AP_Digital_Abuse_Study_Executive_Summary.pdf**

11 Consumer Reports, "Online exposure: Social networks, mobile phones, and scams can threaten your security", June 2011, **http://www.consumerreports.org/cro/magazine-archive/2011/june/electronics-computers/state-of-the-net/online-exposure/index.htm**

12 CNN, "Sexting may not be as widespread as thought, study says", Michael Pearson, December 5, 2011, **http://www.cnn.com/2011/12/05/health/sexting-study/index.html**

Corporate and Sales Headquarters
Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or 408.745.2000
Fax: 408.745.2100
www.juniper.net

APAC Headquarters
Juniper Networks (Hong Kong)
26/F, Cityplaza One
1111 King's Road
Taikoo Shing, Hong Kong
Phone: 852.2332.3636
Fax: 852.2574.7803

EMEA Headquarters
Juniper Networks Ireland
Airside Business Park
Swords, County Dublin, Ireland
Phone: 35.31.8903.600
EMEA Sales: 00800.4586.4737
Fax: 35.31.8903.601

Printed on recycled paper

7100150-001-EN Feb 2012